CURTISS-WRIGHT

Data-At-Rest Encryption Guide

NSA High Assurance Type 1, NSA CSfC, and NIST FIPS 140-2

Trusted. Proven. Leader.

curtisswrightds.com

Data-at-Rest Encryption Solutions

Today's defense and aerospace platforms require the protection of mission-critical data-at-rest (DAR) from unauthorized access. Many of these applications require the use of ready-to-deploy National Institute of Standards and Technology (NIST) or National Security Agency (NSA) approved encryption deployed in a SWaP-optimized solution. Encryption requirements will vary depending on the platform and mission.

As a trusted and proven supplier of SATA and NVMe based rugged storage solutions, Curtiss-Wright offers a wide range of certified COTS network attached storage (NAS) systems. These cost-effective, high-performance solutions incorporate robust data security requirements, including NSA-certified High Assurance Type 1, NSA Commercial Solutions for Classified (CSfC), Common Criteria (CC), and NIST FIPS 140-2. Curtiss-Wright pioneered the development of DAR solutions that provide two layers of CSfC full-disk encryption (FDE) in a single device, with the introduction of the DTS1, the embedded industry's first COTS DAR NAS solution.

In addition to supporting the complete breadth of available encryption methods, Curtiss-Wright's innovative storage products support the following industry-standard NAS protocols (unless otherwise noted):

- File serving: NFS, CIFS, FTP, and HTTP
- Block storage: iSCSI
- Video streaming with real-time protocol: MPEG2 over RTP
- Ethernet recording and packet capture: PCAP
- Remote boot of network clients: PXE and DHCP

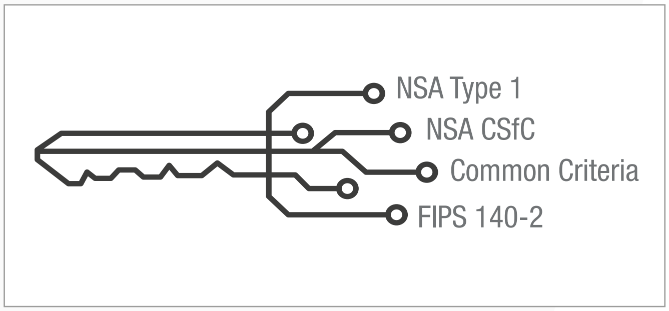


Figure 1: Encryption Standards

To expedite the time to deployment, while reducing the cost of completing CSfC DAR Solution Registration documentation, Curtiss-Wright offers a Compliance Starter Kit (CSK) that includes all the necessary compliance statements for its encryption devices.

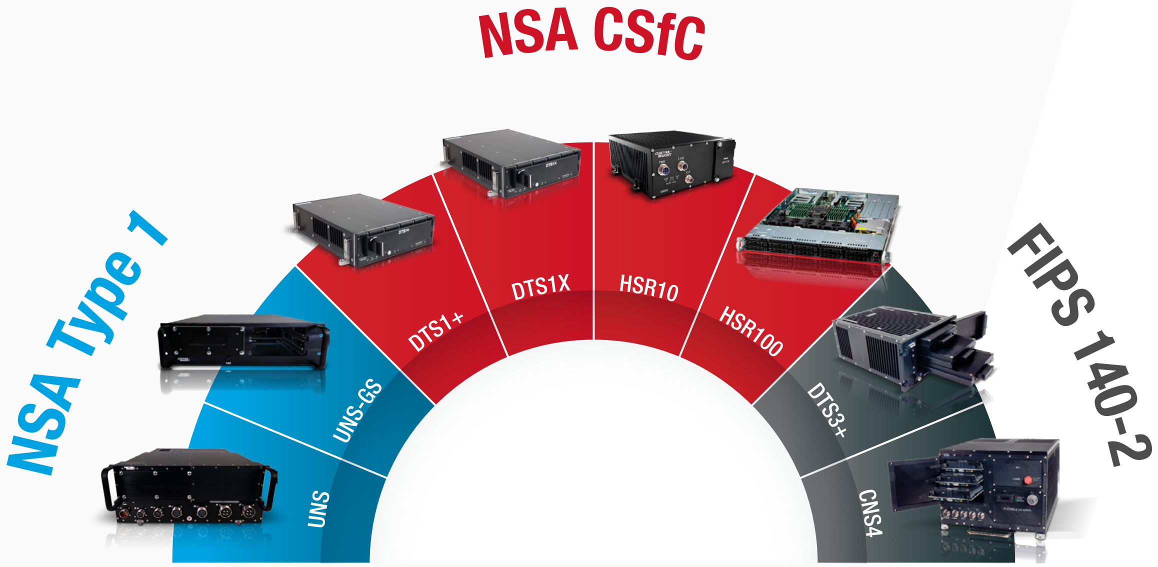


Figure 2: Curtiss-Wright DAR Encryption Solutions

Choosing An Encryption Approach

During missions, deployed vehicles are more susceptible to compromise or loss, which increases threats to DAR. The key to ensuring mission success is to protect classified DAR from both internal and external threats. Nation-states, hackers, and malicious insiders all present significant risks to DAR. Stringent physical security protocols and robust encryption methods must be implemented to safeguard critical data from unauthorized access, exploitation, or loss. Review the risks in the DAR Encryption Series #1: Data Threats and Protection white paper.

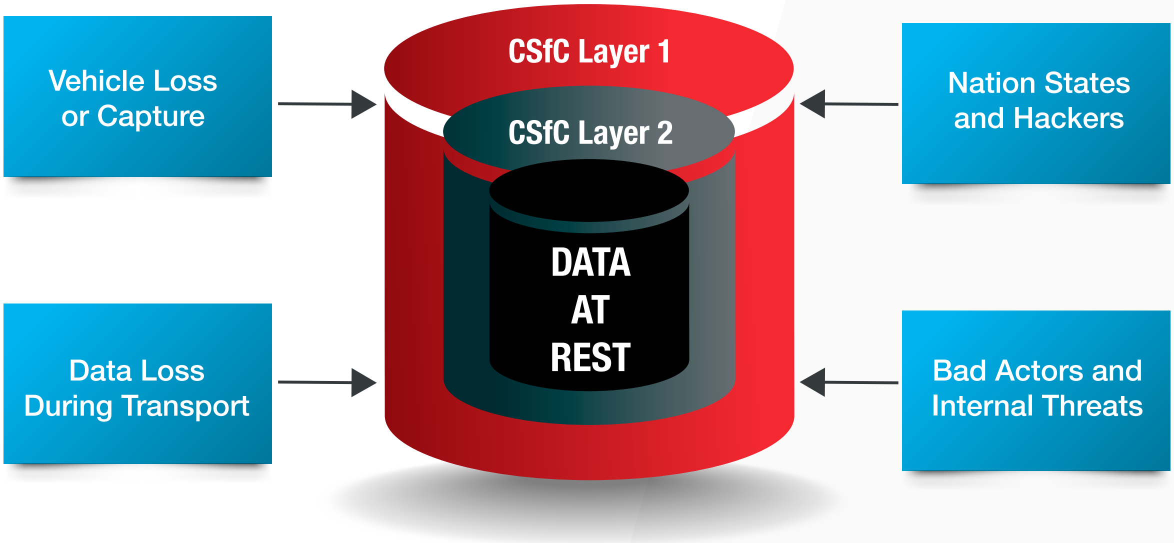

Vehicle Loss or Capture
Data Loss During Transport
CSfC Layer 1
CSfC Layer 2
DATA AT REST
Nation States and Hackers
Bad Actors and Internal Threats

Figure 3: A Two-Layered Approach to Securing Sensitive Data Keeps Data Safe

Adversaries today actively target high-value DAR with harvest now, decrypt later (HNDL) attacks. The intent of the HNDL approach is to obtain encrypted data now while anticipating the availability of future decryption capabilities, such as quantum computing, that will enable the data to be successfully accessed. Learn about quantum cryptographic risks in the Securing Data with Quantum Resistant Algorithms: An Introduction to Post-Quantum Resistant Encryption white paper.

To effectively safeguard classified DAR, it is critical to select the appropriate encryption approach that best meets the needs of the particular target application and platform. Factors such as exportability, data classification levels, encryption layers, technical readiness level, certification duration, cost, and SWaP, must all be evaluated when considering the ideal encryption approach. The NSA sponsors two fundamental DAR encryption approaches, High Assurance Type 1 and CSfC, either of which can be used to protect DAR. Curtiss-Wright, as a leading provider of both High Assurance Type 1 and CSfC NAS solutions, is able to offer a broad and unique perspective to help in the identification and development of an effective DAR protection approach. Read the DAR Encryption Series #4: NSA CSfC vs. High Assurance Type 1 Encryption white paper for an objective, practical, and unbiased comparison between these two NSA programs for encrypting DAR.

While both NSA-sponsored methods, High Assurance Type 1 and CSfC, are commonly used, alternative encryption options, such as those based on Common Criteria (CC) and NIST FIPS 140-2, also offer approaches for evaluating and certifying encryption products, and provide system developers with additional options for satisfying specific security requirements.

NSA CSfC and Common Criteria Encryption

The CSfC program plays a crucial role in the NSA's cybersecurity strategy. CSfC leverages commercial encryption technologies and products in a layered approach to protect classified DAR. Founded on the principle that properly configured, layered solutions will effectively protect classified data in various applications, the adoption of CSfC solutions has accelerated worldwide as system developers recognize the many benefits of commercial encryption technology, including cost-effectiveness and flexibility, compared to traditional approaches.

To provide system developers with the information they need to use COTS solutions to protect critical DAR, the NSA develops, approves, and publishes Capability Packages (CPs) specifications. The NSA also develops and publishes product-level requirements for COTS vendors in United States Government Protection Profiles (PP) aligned with CC. An internationally recognized framework for evaluating and certifying the security features and capabilities of COTS encryption products, CC ensures that solutions meet stringent security requirements for protecting classified DAR.

COTS vendors, such as Curtiss-Wright, make significant investments in Internal Research and Development (IRAD) well ahead of their end customer's requirements to ensure that CSfC components are developed, tested, and approved for inclusion in CSfC solutions.

The NSA CSfC program offers a compelling alternative to the use of traditional High Assurance Type 1 devices to protect classified National Security Systems (NSS) data. The CSfC program enables system developers to minimize development cycles, expedite deployment, and mitigate risk, resulting in a cost-effective option that leverages the latest commercial technology. The DAR Encryption Series #2: Commercial Solutions for Classified (CSfC) white paper provides an in-depth overview of the CSfC program.

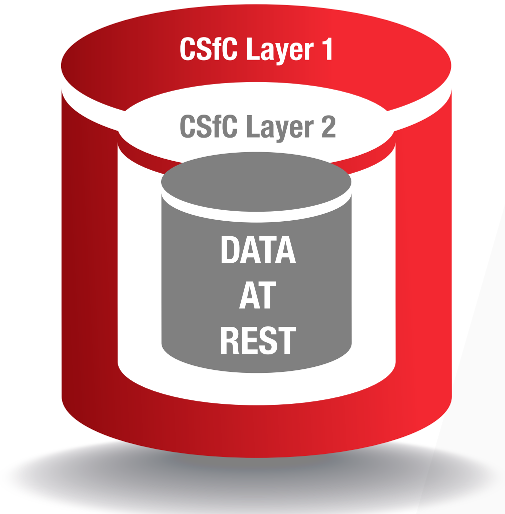


Figure 4: CSfC – Two Layers, One Solution

CURTISS-WRIGHT

DTS1+ 1-Slot Network Attached File Server

The DTS1+ complete turnkey CSfC solution builds on the proven DTS1 DAR NAS solution. It supports two layers of CSfC FDE in a single device. The secure small form factor DTS1+ COTS solution is ready to deploy. With thousands of units already deployed in the field, the DTS1+ is being used to store and protect large amounts of classified data across various applications. With its certified software and hardware encryption layers, the DTS1+ reduces program risk while easing and speeding the ability of system designers to protect DAR with an approved, cost-effective NAS.

The SWaP-optimized DTS1+ weighs only three pounds and occupies less than 50 cubic inches. This rugged NAS can be easily integrated into network-centric systems. It houses one Removable Memory Cartridge (RMC). The NSA designates the RMC as unclassified during transport. The RMC can be easily moved from one DTS1+ into another DTS1+, to enable full, seamless data transfer between networks in separate locations.

DTS1+ Key Features

- NAS with two (2) 1 GbE ports
- Two (2) layers of CSfC FDE
- NSA CSfC Components Listed
- ITAR Free
- SWaP optimized
- Supports TS/SCI for unmanned
- CNSA 2.0 aligned data encryption
- Up to 8 TB of removable storage

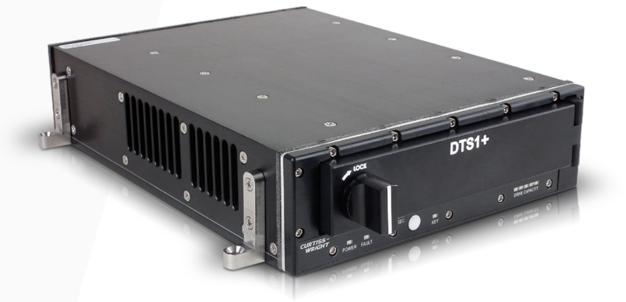


Figure 5: DTS1+ Data Transport System

DTS1X 10 GbE Network Attached Storage

The high-speed DTS1X NAS supports 10 GbE to establish secure, fast data transfer and protect DAR without interrupting or compromising system performance. For 10 GbE architectures that demand high data throughput in SWaP-constrained platforms, the DTS1X NAS provides system developers with an ideal solution. It delivers reliable DAR security with two layers of CSfC-certifiable FDE. The device seamlessly integrates into embedded systems and provides up to 8 TB of removable memory.

DTS1X Key Features

- NAS (one 10 GbE port and one 1 GbE port)
- Two layers FDE
- NSA CSfC Certifiable
- ITAR Free
- SWaP optimized (< 53 cubic inches)
- Up to 8 TB of removable storage

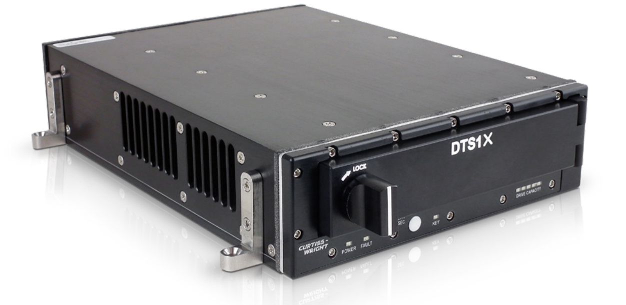


Figure 6: DTS1X Data Transport System

HSR10 10 GbE Network Attached Storage

The HSR10 NAS device features dual 10 GbE ports and two layers of FDE in a single device. Both encryption layers are CSfC certifiable and fully operational in a single chassis to mitigate schedule, cost, and program risk. The HSR10 utilizes the latest NVMe solid-state drive technology for high-speed data throughput and up to 32 TB of removable storage.

HSR10 Key Features

- NAS Two (2) 10 GbE ports and one (1) 1 GbE ports
- Two (2) layers FDE
- NSA CSfC Certifiable
- ITAR Free
- Up to 32 TB of removable storage
- Fast data throughput
  - Write: 1.97 GBps
  - Read: 2.35 GBps

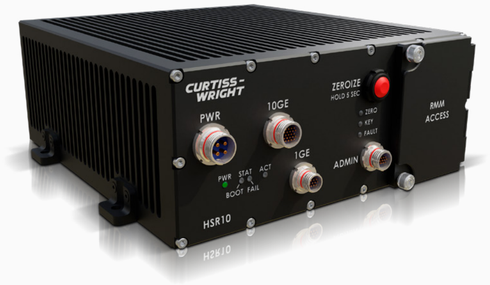


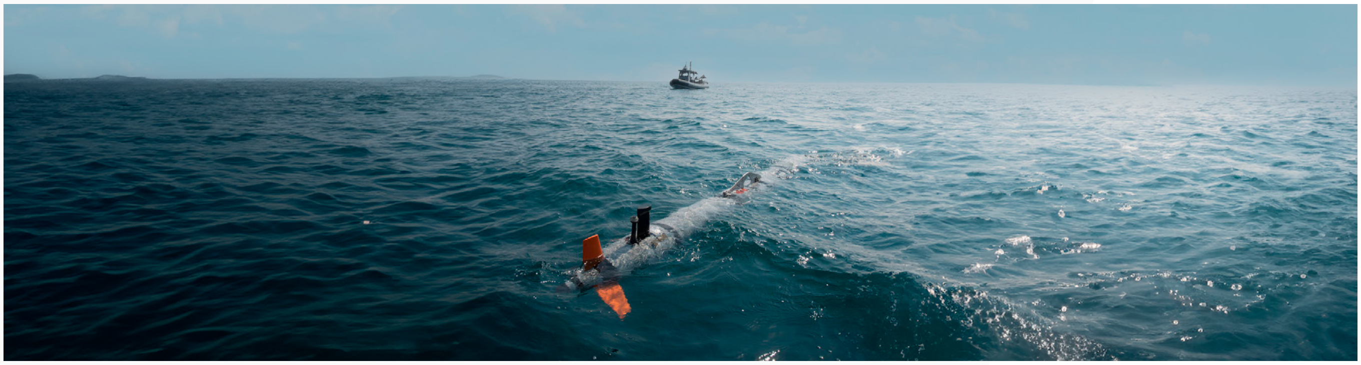
Figure 7: HSR10 CSfC System

CSfC Solution Registration Assistance

An increasing number of programs require the registration of DAR device via the NSA CSfC Solution Registration process. Curtiss-Wright offers the Compliance Starter Kit (CSK) to complement CSfC DAR NAS solutions and to ease and speed completion of CSfC DAR Solution Registration documentation. The CSK helps reduce the time and cost required to complete the Compliance Checklist portion of the Solution Registration process. Since the NSA requires annual CSfC Solution Registration, the benefits of the CSK are ongoing. Use of the CSK reduces recurring costs, such as needing to engage a CSfC Trusted Integrator, typically associated with the annual CSfC DAR Solution Registration process.

NSA-Certified High Assurance Type 1 Encryption

The NSA certifies High Assurance Type 1 products to secure classified U.S. Government information, ranging from Confidential to Secret to Top Secret, when appropriately keyed. The High Assurance Type 1 refers only to products, not information, keys, services, or controls. High Assurance Type 1 products use approved NSA algorithms and are available to U.S. Government users, contractors, and for federally sponsored non-U.S. Government activities, subject to export restrictions per International Traffic in Arms Regulation (ITAR). In addition to the U.S., High Assurance Type 1 devices may also operate in the other Five Eyes countries (U.K., Canada, Australia, and New Zealand). Learn more about NSA-certified High Assurance Type 1 in the DAR Encryption Series #3: High Assurance Type 1 Encryption white paper.



Unattended Network Storage (UNS)

The Curtiss-Wright UNS features the first DAR encryptor certified by the NSA to protect Top Secret and below DAR in unattended operations. It accommodates two General Dynamics Mission Systems High Assurance Type 1 ProtecD@R Multi-Platform Encryptors (KG-204) behind a secured panel. With quad 10 GbE ports for high-speed data throughput, the UNS encrypts incoming data and stores it on the Removable Storage Module (RSM). The RSM is considered unclassified when unpowered and in transport. The UNS keeps data safe from adversaries in forward-deployed locations and autonomous vehicle operations. This rugged and secure, off-the-shelf solution significantly lowers costs and program risk while speeding time to deployment.

UNS Key Features

- Four (4) 10 GbE ports
- Eight (8) 1 GbE ports
- Two (2) High Assurance Type 1 KG-204 encryptors
- One (1) RSM with up to 64 TB of storage capacity

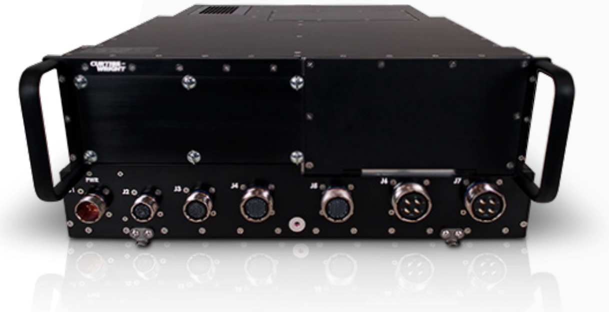


Figure 8: UNS Unattended Network Storage

UNS Ground Station (UNS-GS)

For use with the UNS, the Curtiss-Wright UNS Ground Station (UNS-GS) is designed for deployed vehicles that require High Assurance Type 1 encryption, high-speed data throughput, and high-capacity storage. The UNS-GS accommodates the same RSM used by the UNS. The RSM can be removed from the UNS-GS and safely transported to and from a UNS on a deployed vehicle. The deployed system encryptors encrypt the data files for use during the mission. Post-mission, the RSM can be easily removed for transport back to the UNS-GS to decrypt the captured data and offload it for subsequent analysis.

UNS-GS Key Features

- Four (4) 10 GbE ports and four (4) 1 GbE ports
- One (1) RS-232 port
- Two (2) USB 2.0 ports
- Two (2) NSA High Assurance Type 1 encryption units
- Top Secret and below data protection
- Up to 64 TB removable solid-state memory module
- Up to 2 GBps throughout

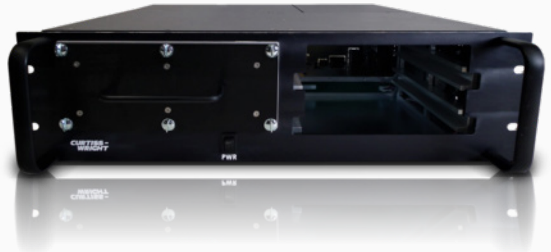


Figure 9: UNS-GS

NIST FIPS 140-2

NIST issues Federal Information Processing Standard (FIPS) Publication 140-2 accredited cryptographic modules. FIPS validated products use the Advanced Encryption Standard (AES) and a 256-bit encryption key to protect sensitive data according to FIPS criteria. FIPS 140-2 is used to safeguard sensitive but unclassified (SBU) information.

DTS3+ 3-Slot Network Attached File Server

The DTS3+ rugged NAS system is designed for mobile vehicles, field ground stations, and aircraft. It supports three removable memory cartridges that deliver seamless data transfer and quick offloading. The DTS3+ supports software full disk encryption (SWFDE), and if hardware full disk encryption (HWFDE) is required, an optional module with three FIPS-certified ASICs is available.

DTS3+ Key Features

- Four (4) 1 GbE ports
- 3 removable memory cartridges
- Up to 2 encryption layers: SWFDE and HWFDE
- Up to 16 TB of storage

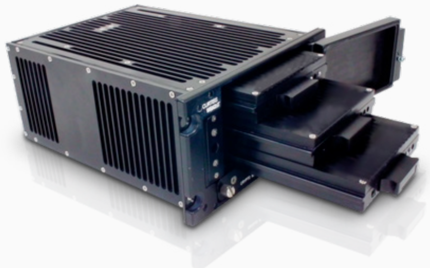


Figure 10: DTS3+ Data Transport System

Compact Network Storage (CNS4): 4-Slot/Non-Certified

For programs with evolving requirements that require flexible storage and FIPS-certified hardware, the CNS4 is offered without CC certification or NSA CSfC approval. Designed with a flexible I/O front end, scalable storage, and advanced encryption options, the CNS4 chassis easily re-configures to meet new or changing requirements while mitigating schedule and budget risks. The flexibility of the CNS4 allows it to serve as a future-proof technology base across multiple platforms.

CNS4 Key Features

- Four (4) 1 GbE ports
- Four (4) FSM-C each with 2 TB of storage capacity
- Protocol support: NAS only (NFS, CIFS, FTP, HTTP)

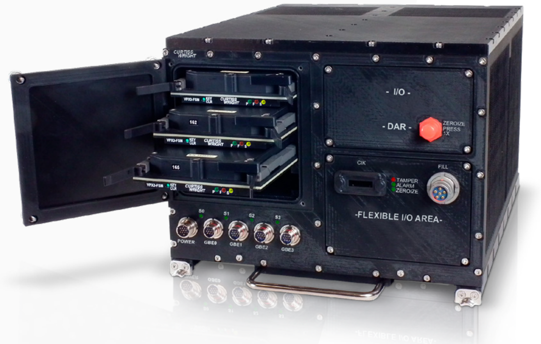


Figure 11: CNS4 Compact Network Storage 4-Slot

HSR100 Rackmount: 100 GbE Secure DAR Storage & Recording

The HSR100 Rackmount supports data storage needs at the platform level. The system ensures data security and availability throughout the mission lifecycle, from mission planning to post-mission data analysis. The HSR100 Rackmount provides secure, network-enabled data storage and recording with two 100 GbE ports, and up to 60 TB of storage. It supports a pathway to NSA CSfC and High Assurance Type 1 encryption.

HSR100 Key Features

- Two (2) 100 GbE and four (4) 10 GbE ports
- Deep learning GPU
- 64 TB of storage
- RAID (0,1,5,10)
- Encryption options available

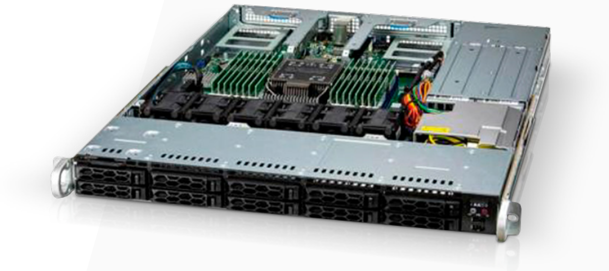


Figure 12: HSR100 Rackmount

	DTS1+	DTS1X	DTS3+	HSR10	UNS	CNS4	HSR100 Rackmount
L x W x H (in)	6.5 x 5.0 x 1.5	7.0 x 5.0 x 1.5	6.5 x 5.0 x 3.0	9.00 x 8.50 x 3.60	18.95 x 17.80 x 7.10	12.50 x 10.00 x 7.62	23.5 x 17.2 x 1.7
Weight (lb)	3.2	3.55	5.5	16.1	<52	39	25
Cubic Inches	48.75	52.5	97.5	275.4	2394.9	952.5	687.1
Network Speed	1 GbE	10 GbE	1 GbE	10 GbE	10 GbE	10 GbE	100 GbE
Encryption	CSfC two layers (HWFDE & SWFDE)	CSfC two layers (HWFDE & SWFDE)	Two layers AES-256	CSfC Up to 2 layers encryption	Type 1	Type 1	None, CSfC & Type 1

Related Content

Products

DTS1+: 1-slot Rugged Network Attached File Server

DTS1X: 10GbE Network Attached Storage

DTS3+: 3-slot Rugged Network Attached File Server

HSR10: 10GbE Network Attached Storage

UNS: Unattended Network Storage

UNS-GS: Network Attached Storage for Unattended Operations

CNS4: 4-slot Rugged Network File Server

HSR100 Rackmount: 100GbE Secure Data Store

White Papers

DAR Encryption Series #1: Data Threats and Protection

DAR Encryption Series #2: NSA Commercial Solutions for Classified (CSfC)

DAR Encryption Series #3: NSA High Assurance Type 1 Encryption

DAR Encryption Series #4: NSA CSfC vs. High Assurance Type 1 Encryption

Securing Data with Quantum Resistant Algorithms: An Introduction to Post-Quantum Resistant Encryption

Securing Data with Quantum Resistant Algorithms: Implementing Data-at-Rest and Data-in-Transit Encryption Solutions

Selecting a High-Speed NAS Device for Military Aircraft

Weighing the Options: SATA vs. NVMe Data Storage for Deployed Applications

Case Studies

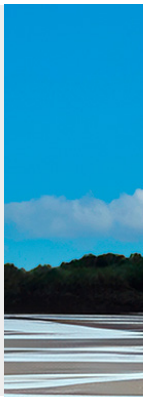
Protecting Data-at-Rest with NSA CSfC Approved Encryption on a UAV

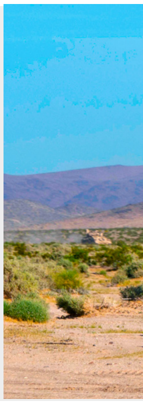
Maximizing Mission Duration and Data Security for UUVs

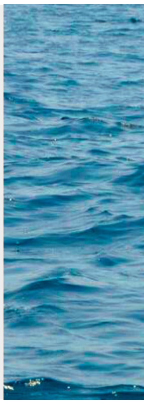
Navigating the Unseen: Mitigating Degraded Visual Environments

Modernizing an ISR Mission with Secure 10 GbE Data Storage

CURTISS-WRIGHT







Contact us

🖥 curtisswrightds.com/sales

✉ ds@curtisswright.com

🌐 curtisswrightds.com